REMARKS

Claims 2-24 are pending in this application. Applicants acknowledge with appreciation that claims 7-20 and 23 contain allowable subject matter[1].

Rejection Under 35 U.S.C. § 101

Claims 2-24 were rejected under 35 U.S.C. § 101 as allegedly being directed to non-statutory subject matter.

For clarification, claim 21 is amended to recite executing, in the electronic device, a set of instructions that is common to the plurality of predefined blocks of instructions a predefined number of times, wherein said predefined number is associated with the selected block of instructions. The subject matter in claim 21 is tied to a particular machine, e.g., the electronic device.

In view of the foregoing, it is respectfully requested that the rejection of claims 2-24 under 35 U.S.C. § 101 be withdrawn.

Rejection Under 35 U.S.C. § 102

Claims 2-6 and 21-24 stand rejected under 35 U.S.C. § 102(b) as anticipated by Kocher (U.S. Patent No. 6,278,783, hereinafter " Kocher"). Applicants respectfully traverse this rejection.

According to exemplary embodiments of the disclosure, in order to execute a chosen block of instructions (π_j) as a function of an input variable (D_i) from N predefined blocks of instructions ($\pi_1, \ldots, \pi_N$), a block (Γ (k,s)) common to the N

[1] In the Office Action, claim 23 is indicated as containing allowable subject matter. See number paragraph 6. However, claim 23 is also rejected under 35 U.S.C. § 102(b). See Office Action: page 4, the fourth paragraph. It is believed that claim 23 contains allowable subject matter. However, if the anticipation rejection of claim 23 was intended by the Examiner when the Office Action was prepared, arguments traversing the anticipation rejection are provided in this Amendment.

predefined blocks of instructions ($\pi_1, \ldots, \pi_N$) is executed a predefined number of times (L_j), the predefined number (L_j) being associated with the chosen block of instructions (π_j).

According to exemplary embodiments of the disclosure, a common block ($\Gamma(k,s)$) can be obtained by performing steps E1-E3:

E1: breaking down each predefined block of instructions ($\pi_1, \ldots, \pi_N$), into a series of elementary blocks γ. For example:

$\pi_1 = \gamma 1 \;||\; \gamma 2 \;||\; \gamma 3$; $\pi_2 = \gamma 4 \;||\; \gamma 5$; ...

For each block of instructions $\pi_1, \ldots, \pi_N$ is broken down thus:

$\pi_1 = \gamma(C_1) \;||\; \ldots \;||\; \gamma(C_1+L_1-1)$

...

$\pi_N = \gamma(C_N) \;||\; \ldots \;||\; \gamma(C_N+L_N-1)$

with

$C_1=0$

$C_2= L_1$

. . .

$C_N= L_1+ \ldots L_N-1$

L_j is the number of elementary blocks necessary for completely breaking down the predefined block of instructions π_j.

E2: seeking a common elementary block ($\gamma(k,s)$) equivalent to all the elementary blocks γ of all the predefined blocks of instructions. For example, a common elementary block γ is sought such that each block of instructions π_j ($1 \leq j \leq N$) can be expressed in the form of a repetition L_j times of the common elementary block γ.

E3: seeking a common block (Γ (k,s)) comprising at least the common elementary block (γ (k,s)) previously obtained during step E2.

Claim 21 recites a method for implementing a cryptographic calculation in an electronic device, comprising the following steps: selecting a block of instructions from amongst a plurality of predefined blocks of instructions, as a function of an input variable; and executing, in the electronic device, a set of instructions that is common to the plurality of predefined blocks of instructions a predefined number of times, wherein said predefined number is associated with the selected block of instructions.

Col. 1, line 66 -col. 2, line 43 and col. 6, lines 28-63, of Kocher, is relied upon in the Office Action as allegedly disclosing the above-recited features of claim 21. Applicants respectfully disagree.

Kocher discloses a masking operation on a message that introduces random state information so that information is invalidated faster than it can be collected by attackers. In Kocher, secrets (e.g., keys and messages) are divided into separate portions, which are separately mutated, while maintaining mathematical relationships among the portions used for performing secure cryptographic operations. In the mutation operation, key management devices introduce randomness into their internal state. The random state information is mixed with the keys, plaintext messages, and intermediate quantities used during processing. As a result, information leaked to attackers during cryptographic processing is correlated to the random information, and any correlation to secret information is partially or completely hidden.

According to Kocher, state parameters are blinded and their order is masked using randomized permutation tables. Specifically, an input message M is blinded to

produce a two-part value (M1, M2). The parameters M1 and M2 are encoded in random order, where permutations M1P and M2P are stored in memory to keep track of the current order of the bits in M1 and M2. M1P and M2P contain bit ordering information and do not represent message content. Neither M1 nor M2 is correlated to the message in any way. Similarly, a key K is blinded to produce a two-part value (K1, K2), and permutations values K1P and K2P are obtained. Permutation values K1P, K2P, M1P, M2P are obtained such that K1P{K1} XOR K2P{K2} equals to the key K, and the M1P{M1} XOR M2P{M2} equals to the plaintext.

Kocher discloses performing masking operations on a message or a key. For example, obtaining the two-part value (M1, M2) of the message M, the two-part value (K1, K2) of the Key K, and obtaining the permutation values (M1P, M2P), and (K1P, K2P), which track of the current order of the bits in M1 and M2, and K1 and K2, respectively. Kocher does not disclose performing masking operations on executable instructions. In contrast, claim 21 recites selecting a block of instructions from amongst a plurality of predefined blocks of instructions, as a function of an input variable; and executing, in the electronic device, a set of instructions that is common to the plurality of predefined blocks of instructions a predefined number of times, wherein said predefined number is associated with the selected block of instructions. Therefore, Kocher fails to disclose that attacks on a the cryptographic calculation can be thwarted by manipulating executable instructions, as described in claim 21.

Furthermore, according to claim 21, the cryptographic calculation includes executing a set of instructions that is common to the plurality of predefined blocks of instructions a predefined number of times, wherein said predefined number is

associated with the selected block of instructions. Since Kocher lacks disclosure on manipulation of instructions, Kocher does not teach or suggest executing a set of instructions that is common to the plurality of predefined blocks of instructions. More specifically, Kocher does not teach or suggest executing a set of instructions that is common to the plurality of predefined blocks of instructions a predefined number of times, wherein said predefined number is associated with the selected block of instructions.

In view of the foregoing, claim 21 is patentable. Claims 2-6 and 22-24 are patentable at least because of their dependency from claim 21.

Allowable Subject Matter

Applicant acknowledges with appreciation that claims 7-20 and 23 contain allowable subject matter. Since the base claim and intervening claims are believed to be patentable, claims 7-20 and 23 are in condition for allowance.

Conclusion

For the foregoing reasons, Applicants respectfully submit that this application is in immediate condition for allowance and all pending claims are patentably distinct from the cited references. Reconsideration and allowance of all pending claims are respectfully requested.

In the event that there are any questions about this application, the Examiner is requested to telephone Applicants' undersigned representative so that prosecution of the application may be expedited.

If additional fees are required for any reason, please charge Deposit Account No. 02-4800 the necessary amount.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: August 31, 2009

By: Weiwei Y. Stiltner
Weiwei Y. Stiltner
Registration No. 62,979

P.O. Box 1404
Alexandria, VA 22313-1404
703 836 6620

Customer No. 21839